Issues In Internet Commerce

Thomas E. Jensen[(1)]

Growth of the Internet has exploded, with expectations of even greater increases in use. With a marketplace estimated in the tens of millions, it's no wonder commercial uses have also burgeoned. Publishing a Web page is an excellent way for any business to vastly increase its exposure to millions of individuals world-wide. It is that feature of the Internet which is causing much controversy in the legal community. This article will explore some of the issues which threaten to undermine the viability of the Internet for commercial use.[(2)]

The Domain Name Controversy.

Once a business decides to go "on-line," it must obtain a "domain name" to provide access to its Web page through its Internet computer. Generally speaking, domain names are not difficult to obtain, but getting a domain name closely related to the business name, logotype, trademark, or service mark could be problematic.

A domain name is an address for a particular computer connected to the Internet through which information is transferred to or from the owner of a particular Web page, and others. To avoid communication errors, each address must be unique. Accordingly, Internet domain names are assigned, on a first-come, first-served basis, by registering with the Internet Network Information Center of the National Science Foundation ("InterNIC"). Registration is administered by Network Solutions Inc. ("NSI"), a Virginia company under contract with InterNIC.[(3)]

Domain names have two elements: A "top-level" domain, and a "second-level" domain. There are presently six top-level domains in the U. S. -- *.com; .edu; .gov; .mil; .org;* and *.net*.[(4)] To complete the domain name the so-called second-level domain is added as a prefix to the top-level domain, such as a company name, acronym, abbreviation, service mark, or trademark.

The domain name is not, however, a service mark or a trademark. Therein lies the problem. In several cases long-established trademarks have been registered as domain names by individuals with no relationship to the trademark owner. Some have been instances of clever marketing by "innocent" parties and are usually resolved quickly. Others, where the owner of the domain name bargains to release it to the trademark owner for a monetary settlement, have questionable motives. These "cybersquatters" essentially circumvent the use of its trademark on the Internet by the rightful owner. This ruse may be short-lived.

The Central District of California recently granted summary judgment to plaintiff Panavision against an Illinois cybersquatter who had registered both its trademarks "Panavision" and "Panaflex" as domain names *panavision.com* and *panaflex.com*.[(5)] The court found the action of the defendant -- registering

trademarks as domain names and then selling them to the trademark owners -- was a "dilutive' commercial use in violation of the Federal Trademark Dilution Act.(6) Similarly, the U. S. District Court for the Northern District of Illinois granted summary judgment for plaintiff in *Intermatic Inc. v. Toeppen*, finding dilution because the defendant's registration and use of Intermatic's name as his domain name would lessen Intermatic's ability to identify and distinguish its goods and services on the Internet.(7) Future issues of trademark infringement via domain name registration may be resolved using the federal law. However, disputes over domain name registration are sure to continue as the number of Internet users grows.

Domain name registration made NSI the focus of several lawsuits.(8) In response, NSI adapted its registration policies. In September NSI published the most recent version of its registration policies, including new third-party dispute resolution procedures.(9) The new policy essentially gives the nod to prior registrations, whether domain names or trademarks. Thus, under NSI's dispute resolution policy, trademarks registered prior to domain names will have preference, while domain names registered prior to trademarks will prevail -- and where either party withholds information required to determine registration dates, NSI will place the challenged domain name on "hold," denying its use to either party until a court determines the rights to the domain name.(10)

This new area of law is just beginning to evolve. To reduce future concerns over rights to trademarks or domain names, a business should search both domain names and trademarks before applying for its own domain name. If a business wants to protect its future use of a domain name, it should register its trademark as its domain name, or its domain name as its trademark.

Developments In Jurisdiction.

Businesses engaging, or contemplating engaging, in commerce on the Internet should pay close attention to issues of jurisdiction, and the impact use of the Internet may have on its exposure to lawsuits in remote forums. The cases appear inconsistent, but a trend seems to be developing.

In the case of *Inset Systems Inc. v. Instruction Set Inc.*(11) defendant Instruction Set Inc. ("ISI"), a Massachusetts computer technology company, had neither an office nor employees in Connecticut, and did not regularly conduct business there. However, the Federal District Court held that ISI was subject to jurisdiction in Connecticut because it had purposefully availed itself of the privilege of doing business in Connecticut by advertising on a Web page accessible to residents of Connecticut using the name "Inset," which plaintiff, a software marketing company, had trademarked, and by providing a toll-free telephone number "1-800-US-INSET," which could be used by Connecticut residents to contact defendant. The U. S. District Court in Connecticut also imposed jurisdiction in Connecticut against a California resident accused of fraudulent stock sales in *Cody v. Ward*,(12) where the defendant's actions to induce plaintiff to purchase stock through e-mail and the telephone were sufficient contacts with Connecticut to sustain jurisdiction even though defendant had no other contacts with the state. Furthermore, defendant's conduct in Connecticut was enough to purposefully establish contact with the forum state that he should reasonably anticipate being haled into court there.

The U. S. District Court for the Eastern District of Missouri followed the *Inset* decision in *Maritz Inc. v. Cybergold Inc.*,[(13)] also a trademark infringement action. The court held that defendant was properly subject to jurisdiction in Missouri because it used its Berkeley, California, interactive Web site to solicit Internet users, including 131 transmissions to Missouri, for its mailing list.

In *Hall v. LaRonde*[(14)], a contract action, the California Court of Appeal held a New York software consultant was amenable to suit by a California software developer because the defendant's activities with the plaintiff, who reached out to New York by e-mail, involved "reaching back" to California by e-mail and telephone. In *Telco Communications V. An Apple A Day*,[(15)] the U. S. District Court for the Eastern District of Virginia upheld jurisdiction in a defamation action, brought in Virginia against a Missouri telemarketer, finding that defendant engaged in a persistent course of conduct in Virginia by posting the defamatory press releases on the Internet, that the tort would not have occurred in Virginia but for the Internet, and that the defendant could reasonably have anticipated that the press releases would be disseminated in Virginia, where TELCO is based. In other words, use of the Internet resulted in the locus of the tort being Virginia, where and numerous affected investors could have access to the disputed press releases and plaintiff was injured.

Recently, the Sixth Circuit Court of Appeals in Ohio held that a Texas software distributor, who had contracted with CompuServe, Inc. in Ohio to distribute his software over the Internet on CompuServe's computer, had by that action purposefully availed himself of the privilege of conducting business in Ohio, and that his later allegations that CompuServe infringed that software rightfully subjected him to jurisdiction in Ohio.[(16)]

These cases all involved some activity on the part of the defendant in the forum state. It appears that having a Web page accessible by users in remote forums probably won't be enough by itself to confer personal jurisdiction. In *McDonough v. Fallon McElligot*,[(17)] the U. S. District Court for the Southern District of California held that merely having a Web site, without more, is insufficient to confer jurisdiction. And the U. S. District Court for the Southern District of New York held, in *Bensusan Restaurant Inc. v. Richard B. King*,[(18)] that the mere existence of a Web site was not enough to impose jurisdiction in New York on a Missouri defendant. Bensusan operated a jazz club in New York under the a federally registered trademark "The Blue Note." King operated a small club in Columbia, Missouri, also called "The Blue Note." To promote his club, King posted a Web site on a computer located in Missouri, containing a logo substantially the same as plaintiff's logo. King's Web site contained general information about his club, with a calendar of events and ticketing information. The court found that because King's show tickets could only be purchased in Missouri, any trademark "confusion" with Bensusan's New York club would occur there, not in New York. The court pointed out King had disclaimed association with The Blue Note in New York, had done nothing to purposefully avail himself of the benefits of New York, and it would violate due process to assert personal jurisdiction based on the maintenance of a Web site. The court distinguished *CompuServe, supra*, by the fact Patterson had specifically targeted Ohio by subscribing to and using CompuServe's service to distribute his software, had advertised his software through the service, and had repeatedly sent his software to the service in

Ohio, "reaching out" from Texas to Ohio.

The *Bensusan* decision was followed by the 9th Circuit Court of Appeals in *Cybersell, Inc.Arizona v. Cybersell, Inc. Florida*,(19) where the court decided it would not comport with traditional notions of fair play and substantial justice for Arizona to exercise personal jurisdiction over an allegedly infringing Florida web site advertiser who has not contacts with Arizona other than maintaining a home page accessible to Arizonans, and everyone else, over the Internet. The court distinguished *Maritz v. Cybergold*,(20) and *Inset Systems Inc. v. Instruction Set, Inc.*(21) by the nature and quality of the commercial activity the entity conducted over the Internet. Unlike the defendants in those cases, *Cybersell, Inc Florida* conducted no commercial activity over the Internet in Arizona with its passive Web page.

A Minnesota court recently aimed at the interactive activity of a Nevada Web site which could be accessed by computers in Minnesota. In *State of Minnesota v. Granite Gate Resorts*, the court denied defendant's motion to dismiss for lack of jurisdiction after reviewing the number of "hits" received on defendant's computer from Minnesota, considering the toll-free telephone number advertised on the Web page, and counting the number of Minnesota residents who had signed on to defendant's mailing list.(22)

The court evaluated the Internet activity under Minnesota's five-factor test for imposing personal jurisdiction,(23) and held that advertising on the Internet constituted a direct marketing campaign to the state of Minnesota(24) which, in light of the interaction with computers in the forum state, was sufficiently purposeful to subject the defendant to suit in Minnesota.(25)

While courts seem to require individuals to conduct some activity with the forum to support personal jurisdiction, the extent of that activity is hard to define. It seems that the requirement for activity is satisfied when some "interaction" is found between the Web site and residents of the forum state. This raises the question how that interaction might take place. Given the prevalence and utility of *hyperlinks*,(26) it is uncertain whether unknown and unsuspected links from one Web page to another could create sufficient "interactions" to support jurisdiction over the owner of the linked site.

Extra-Territorial Application of State Laws.

Aside from the finding of jurisdiction over a Nevada defendant in Minnesota, the

Granite Gate Resorts case is significant because the court upheld the Minnesota Attorney General's authority to seek to enjoin the defendant's Internet activities under Minnesota laws prohibiting gambling, deceptive trade practices, false advertising, and consumer fraud. Defendant Granite Gate Resorts is not only being haled into court in Minnesota, but is being prosecuted under Minnesota law based on solicitations in Nevada reaching Minnesota on the Internet. Minnesota is not the only state purporting to impose its laws on Internet conduct in other states.

California recently enacted a law which specifically extends to out-of-state vendors using the Internet to advertise, sell, or lease, goods or services.(27) Section 17538 of the Business & Professions Code was

amended to add, to telephone, mail order or catalogue sales, leases, or offers of sales and leases "in this state," similar activities by use of the Internet, "or other electronic means of communication or telecommunications device"(28) when engaging in one or more transactions aggregating more than ten dollars.(29) Application of this law to vendors outside California is clearly intended: it requires vendors, including those using the Internet or other electronic means of communication to provide specific refund and return policies,(30) and certain disclosures, to buyers in California.(31) Since Web pages are viewed world-wide, this law essentially attempts to impose requirements on vendors wherever located if any buyer resides in California. Although the law encompasses solicitations as well as sales, given the need for "interactions" discussed above, jurisdiction to enforce its provisions on a remote Internet seller will probably require purchases by California residents.

The ACLU has challenged a law recently enacted by the state of Georgia, which was intended to prevent the Internet use of pseudonyms or aliases ("falsely identify"), or posting logos or trademarked images to "falsely imply" authority to use the image.(32) Though the ACLU challenge rests on Constitutional principles of free speech and privacy, enforcement of the Georgia law threatens to alter use of *hyperlinked* objects, and the anonymity of Newsgroups and so-called "chat-rooms."(33)

Extra-territorial application of state law has the potential to seriously undermine the utility of Internet commerce. It is difficult enough to comply with all applicable laws when intentionally marketing to buyers in other states, but the necessity of adapting to the demands of each of the fifty states (and other countries) merely because the business uses the Internet could lead to significant unexpected burdens and liabilities on business in Internet commerce. Such a burden may ultimately lead to federal regulation of Internet activity.

To avoid inadvertent applicability of other state's laws, the business planning to use the Internet should take meaningful steps, and make continuing efforts, to control the scope of its "interactions" with other forums. Since advertising on the Internet can't realistically be limited geographically, the business itself must clearly limit its geographical market area through appropriate notices on its Web page. More than notices, though, the business must make every effort to decline all transactions arising from a location outside its defined market.

Special Problems For Financial Institutions.

Financial institutions are required under the Bank Secrecy Act(34) to monitor certain financial transactions and to file reports, such as for currency transactions and so-called "suspicious activity." Transactions over the Internet are already targeted for scrutiny by the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") since the efficiency and anonymity of such transactions make them attractive tools for money-laundering. FinCEN refers to these transactions as "cyberpayments," and views the transfer of "financial value" over the Internet with suspicion.(35) FinCEN has expressed concern as to how financial institutions will be able to continue to provide effective money-laundering information as face-to-face transactions decrease in favor of on-line banking.(36)

Accepting deposits through cyberpayments may require financial institutions to alter their existing policies for customer identification. If a financial institution suspects a transaction, the amount and type of information it must report on a Suspicious Activity Report ("SAR")[(37)] clearly contemplates a face-to-face transaction (e.g., full name, address, date of birth, occupation, I. D. -- driver's license, passport, alien registration card -- number, relationship to the institution, and to other institutions). Since this information is unlikely to be reliably obtained over the Internet at the time of the suspicious transaction, it would have to be collected when the relationship is first established and, to guard against falsification, its accuracy should be independently verified at the remote location to enable the institution to meet its reporting obligations.

Internet use could also impact a bank's regulatory compliance efforts. A bank is required to define its market area, and to provide information about deposits and loans to enable regulators to monitor for evidence of discrimination in credit under such laws as the Home Mortgage Disclosure Act ("HMDA")[(38)] and performance under the Community Reinvestment Act ("CRA").[(39)] For example, the CRA requires banks to establish market areas contiguous to their branch offices, and to map them using existing boundaries, such as Standard Metropolitan Statistical Areas ("SMSAs") or counties, in which the offices are located.[(40)] What standard would a successful "cyberbank" use to delineate its community? It is uncertain whether the FRB would permit a written description of a "cybercommunity" for Internet customers similar to the "military community" permitted for banks whose market area includes mobile military families.[(41)]

Proceed With Caution.

Presented with the potential of the Internet, any business without its own Web page might be tempted to move quickly to get "on-line." That might be a mistake, however. Blindly exposing one's business to the consequences of uncertain jurisdiction, or to the unexpected application of another state's laws, could be a recipe for disaster. Even so -- it is tempting.

If a business plans to go "on-line," it should protect its trademark and future domain name by taking a few preliminary measures. First, search both domain names and trademarks. If its trademark is already registered as a domain name, it could initiate third-party dispute resolution procedures with NSI to stop the infringing use. If its trademark isn't a domain name, the business should register it as such to prevent subsequent use by others and future litigation. If the business wants to use another symbol as a domain name which is not already registered, it should do a trademark search to ensure it won't infringe another's mark. If the coast is clear, register the symbol as both a domain name and a trademark.

Since interactions with a remote forum are the seeds of jurisdiction, it's important to avoid unintended interactions. Design the Web page with special attention to the business' defined market area. In addition to a well-defined and limited market area clear on the face of the Web page, the business should establish firm procedures designed to identify transactions originating from outside the defined market -- and to deny them.

Traditional concepts of jurisdiction and territorial legal boundaries are being stretched in cyberspace. There is an obvious need for a stable legal environment in which to conduct electronic commerce. Arguably, no business using the Internet should be held hostage to uncertain jurisdiction, or the application of other states' laws. On the other hand, no individual consumer should be left without a remedy just because he or she was a victim of a "cyberscam" on the Internet. It is certain the growth of the Internet will challenge both courts and legislatures as they wrestle with new, truly global, issues.

NOTES:

1. Thomas E. Jensen is principal of Lender Compliance Services in Escondido, California. Mr. Jensen is a member of the consumer Financial Services Committee of the Business Law Section. **This article is updated and accurate as of December 21, 1997.**

2. A number of states -- including California -- have recently passed laws prohibiting pornography, especially child pornography, over the Internet. However, the controversial issues raised by such laws are beyond the scope of this article, which is limited to issues arising out of commercial use.

3. NSI contracted with InterNIC to register domain names through the Spring of 1988, after which time InterNIC has indicated it will no longer be involved in domain name registration. Instead, top level domains will be registered by the Council of Registrars ("CORE") established under the IAHC gTLD-MOU signed on May 1, 1997 (*see*, note 4, *infra*).

4. Top-level domains now in userepresent the following: *.com* for commercial use; *.edu* for educational institutions; *.gov* for government use; *.mil* for military use; *.org* for non-profit organizations; and *.net* for administration of other networks. With increasing use of *.com*, on February 4, 1997 seven additional top-level domain names were proposed, and on May 1, 1997 approved, by the International Ad Hoc Committee ("IAHC"). The IAHC, consisting of the Internet Society (ISOC), Internet Assigned Numbers Authority (IANA), Internet Architecture Board (IAB), Federal Networking Council (FNC), International Telecommunication Union (ITU), International Trademark Association (INTA), and World Intellectual Property Organization (WIPO), was disbanded on May 1, 1997 upon the adoption of the gTLD-MOU memorandum of understanding which, by December 15, 1997, had garnered 188 signatories.

The new top-level domains proposed by the IAHC are: *.firm* for businesses or firms; *.shop* for businesses offering goods to purchase; *.web* for entities emphasizing activities related to the World Wide Web; *.arts* for entities emphasizing cultural and entertainment activities; *.rec* for entities emphasizing recreational/entertainment activities; *.info* for entities providing information services; and *.nom* for those

wishing individual or personal nomenclature, i.e., a personal *nom de plume*.

These domains are "generic" top-level domains ("gTLD"). Other domains are national domains ("nTLD"), relating to country codes such as *.au* for Australia, *.us* for the United States, and *.ch* for Switzerland, for example, and international domains ("iTLD"), relating to entities which have a truly international character, e.g. *.int*, which includes, among others, international intergovernmental organizations.

The gTLD-MOU only applies to registration of the seven new top-level domains, however. If InterNIC abandons domain name registrations without renewing its contract with NSI, by Spring of 1998 only the seven new top-level domains will be in use. Registration of the new top-level domains will begin in early 1998.

Information on how to become a registrar of domain names, and an application form, may be obtained from "www.gtld-mou.org/docs/application.htm."

5. *Panavision v. Toeppen*, 938 F.Supp. 616 (C. D. Cal. 1996).

6. 15 U.S.C. 1125(c).

7. 947 F,Supp. 1227 (N. D. Ill. Oct. 3, 1996).

8. *Giacalone (ty.com) v. NSI*, U. S. District Court for the Northern District of California, San Jose Division, Case No. C-96-20434; *Data Concepts, Inc. v. NSI*, where a stipulation and order were entered May 24, 1996 to prevent NSI from interrupting Data Concept's use of the domain name *dci.com*; *Roadrunner Computer Systems, Inc. v. NSI*, U. S. District Court for the Eastern District of Virginia, Civ. 96-413-A, was dismissed as moot on June 21, 1996; *Clue Computing Inc. v. NSI*, where Hasbro Toys is challenging Clue Computer's use of the domain name *clue.com*.

9. Network Solutions Inc. "Domain Name Dispute Policy," effective September 6, 1996.

10. *Id.* At Section 6. A new dispute resolution procedure was proposed by the IAHC in the gTLD-MOU and the CORE-MOU, which call for mandatory, non-binding, mediation without depriving the parties of the use of the judicial system in the country of registration. The premise is that a domain subject to challenge would not be able to be used until the dispute is resolved. More information on this procedure may be obtained at "www.gtld-mou.org."

11. 937 F.Supp. 161 (D. Conn. 1996).

12. Case No. 3:95CV169(RNC), (DC CT Feb. 4, 1997).

13. BNA Electronic Information Policy & Law Report, Vol. 1 at 587, No. 4:96CV01340 (E. D. Mo. Aug. 19, 1996).

14. 66 Cal. Rptr. 2d 399, (Cal. App. 2d Dist. Aug. 7, 1997). The court noted that physical presence in the forum state should not be determinative, and that there is no reason why the requisite minimum contacts cannot be electronic.

15. Civil Act. No. 97-5542-A (DC VA Sept. 24, 1997).

16. *CompuServe v. Patterson & Flashpoint Development*, 89 F.3d 1257 (July 22, 1996).

17. Civ. 95-4037 (S. D. Cal. Aug. 5, 1996).

18. 937 F.Supp. 295 (S. D. N. Y. Sept. 9, 1996); *aff'd.* Docket No. 96-9344 (US CA 2d Sept. 10, 1997).

19. 97 C.D.O.S. 9006; D. C. No. CV-96-00089-EHC (US CA 9th Dec. 2, 1997).

20. 947 F. Supp. 1328 (E. D. Mo.), *see* note 13, *supra*.

21. 937 F. Supp. 161 (D. Conn. 1996), *see*, note 11, *supra*.

22. Ramsey County District Court File No. C-6-95-7227, Dec. 11, 1996; *aff'd.* C6-97-89 (CA MN Sept. 15, 1997). The memorandum of decision by the trial court may be obtained through the following URL:

http://www.ljestra.com/cgi-bin/f_cat?prod/ljextra/data/external/1996/07/9607037.c06.

The appellate decision may be obtained at:

http://www.courts.state.mn.us/opinions/coa/current/c69789.html.

23. *Id.* Memorandum of Decision, page 6, recites the five factors to be considered:

1. The quantity of contacts with the forum.

2. The nature and quality of those contacts.

3. The connection of the cause of action with the contacts.

4. The interest of the state in providing a forum.

5. The convenience of the parties.

24. *Id.* At page 7.

25. *Id.* At page 11.

26. A *hyperlink* is a symbol or highlighted text in a Web page which permits "jumps" to other pages of the same document, or to other Web sites, often without the knowledge (or consent) of the owner of the linked site.

27. Assembly Bill 3320, filed with the Secretary of State Sept. 23, 1996, as Chapter 785 of the Statutes of 1996, effective January 1, 1997.

28. B&P 17538(a). Inclusion of the phrase "other electronic means of communication or telecommunications device" ensures the law applies to all forms of such communication, whether on the Internet, the World Wide Web, a Local or Wide Area Network, or closed electronic communication network. The phrase is undefined in the law, and presumably would also reach sales and solicitations at electronic terminals, such as Automated Teller Machines, and others.

29. *Id.* At (e)(5). The term "vendor" is defined to exclude those providing goods or services if the aggregate amount of all transactions does not exceed ten dollars.

30. *Id.* At (a)(2) through (4). The vendor generally must either mail a full refund or ship substitute goods if more than 30 days elapses from the time payment is received.

31. *Id*. At (d), which reads:

A vendor conducting business through the Internet, or any other means of electronic communication shall do all of the following when the transaction involves a buyer in California:

(1) Before accepting payment or processing any debit or credit charge or funds transfer, the vendor shall disclose to the buyer in writing or by electronic means of communication, such as e-mail or on-screen notice, the vendor's return and refund policy, the legal name under which the business is actually conducted and, except as provided in paragraph (3), the complete street address from which the business is actually conducted.

(2) If the disclosure of the vendor's legal name and address required by this subdivision is made by on-screen notice, all of the following shall apply:

(A) The disclosures of the legal name and address information shall appear on any of the following: (i) the first screen displayed when the vendor's electronic site is first accessed, (ii) on the screen on which the goods or services are first offered, (iii) on the screen on which the buyer may enter the order for the goods or services, or (iv) on the screen on which the buyer may enter payment information, such as a credit card account number. The communication of that disclosure shall not be structured to be smaller than the text of the offer of the goods or services.

(B) The disclosure of the legal name and address information shall be accompanied by an adjacent statement describing how the buyer may receive the information at the buyer's e-mail address. The vendor shall provide the disclosure information at the buyer's request.

(C) Until the vendor complies with subdivision (a) in connection with all buyers of the vendors' goods and services, the vendor shall make available to buyer and any person or entity who may enforce this section pursuant to Section 17535 on-screen access to the information required to be disclosed under this subdivision.

(3) The complete street address need not be disclosed as required by paragraph (1) if the vendor utilizes a private mailbox receiving service and all of the following conditions are met: (A) the vendor satisfies the conditions described in paragraph (2) of subdivision (b) of Section 17538.5; (B) the vendor discloses the actual street address of the private mailbox receiving service in the manner prescribed by this subdivision for the disclosure of the vendor's actual street address; and (C) the vendor and the private mailbox receiving service comply with all the requirements of subdivisions (c) through (f), inclusive, of Section 17538.5.

32. *ACLU of Georgia v. Miller*, 96-2475.

33. Newsgroups and chat-rooms are Internet communications services where individuals with similar interests can communicate. The anonymity of those communications is a prime feature of the service.

34. 12 U.S.C. 1951, *et seq.*, implemented by the Department of Treasury's Financial Recordkeeping and Reporting of Currency and Foreign Transactions Regulation, 31 C.F.R. 103, *et seq.*

35. *See* the Frequently Asked Questions ("FAQ") at the FinCEN Web page, which can be accessed at the Uniform Resource Locator ("URL") http://www.ustreas.gov/treasury/bureaus/fincen/cypage.html. FinCEN defines the term "cyberpayments" to include the transfer of financial value over the Internet or by stored-value cards. FinCEN is concerned because, it notes, cyberpayments have the potential to facilitate the international movement of illicit funds.

36. *Id.*, at FAQ "What are some of law enforcement's specific concerns?" -- *The Impact of Traditional Investigation and Analysis.*

37. FRB form FR 2230 (OMB No. 7100-0212), expires September 30, 1998.

38. 12 U.S.C. 2801, *et* seq., implemented by FRB Regulation C, 12 C.F.R. 203, *et seq.*

39. 12 U.S.C. 2901, *et seq.*, implemented by FRB Regulation BB, 12 C.F.R. 228, *et seq.*

40. CRA requires banks to delineate their community, and at least annually to review their entire community, using maps to portray community delineations. 12 C.F.R. 228.3(a).

41. A military community may be delineated by a written description rather than a map. *Id.*, at (c).